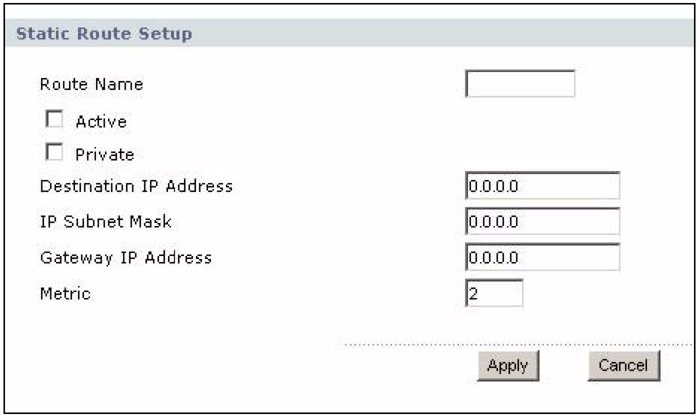
Figure 84 Management > Static Route > IP Static Route > Edit



Static Route Setup

Route Name	
□ Active	
□ Private	
Destination IP Address	0.0.0.0
IP Subnet Mask	0.0.0.0
Gateway IP Address	0.0.0.0
Metric	2

Each field is described in the following table.

Table 49 Management > Static Route > IP Static Route > Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the static route.
Active	Select this if you want the static route to be used. Clear this if you do not want the static route to be used.
Private	Select this if you do not want the ZyXEL Device to tell other routers about this static route. For example, you might select this if the static route is in your LAN. Clear this if you want the ZyXEL Device to tell other routers about this static route.
Destination IP Address	Enter one of the destination IP addresses that this static route affects.
IP Subnet Mask	Enter the subnet mask that defines the range of destination IP addresses that this static route affects. If this static route affects only one IP address, enter 255.255.255.255.
Gateway IP Address	Enter the IP address of the gateway to which the ZyXEL Device should send packets for the specified **Destination**. The gateway is a router or a switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Usually, you should keep the default value. This field is related to RIP. See Chapter 8 on page 83 for more information. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". The smaller the metric, the lower the "cost". RIP uses hop count as the measurement of cost, where 1 is for a directly-connected network. The metric must be 1-15; if you use a value higher than 15, the routers assume the link is down.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to return to the previous screen without saving your changes.

CHAPTER 16
Remote MGMT

Use these screens to control which computers can use which services to access the ZyXEL Device on each interface.

16.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which ZyXEL Device interface (if any) from which computers.

You may manage your ZyXEL Device from a remote location via:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable).

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1 Telnet
2 HTTP

16.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2 You have disabled that service in one of the remote management screens.
3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.
4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

16.1.2 Remote Management and NAT

When NAT is enabled:

- Use the ZyXEL Device's WAN IP address when configuring from the WAN.
- Use the ZyXEL Device's LAN IP address when configuring from the LAN.

16.1.3 System Timeout

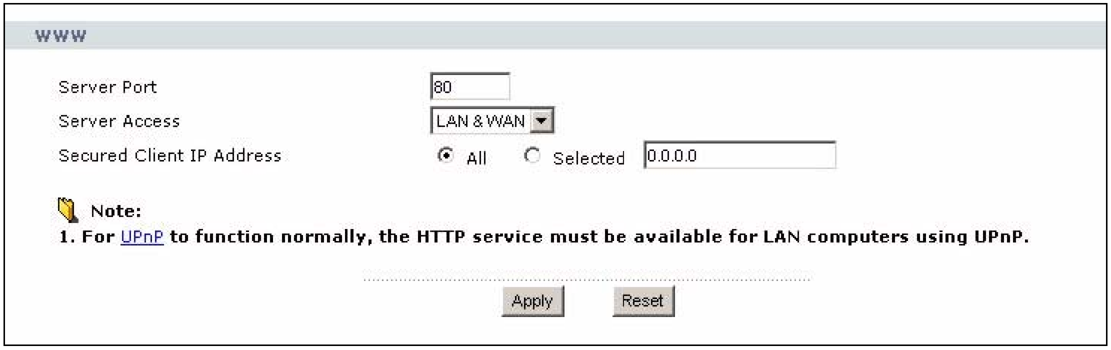
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **Maintenance > System > General** screen.

16.2 Remote Management Screens

16.2.1 WWW Screen

Use this screen to control HTTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > WWW**.

Figure 85 Management > Remote MGMT > WWW



WWW

Server Port: 80

Server Access: LAN & WAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Note:
1. For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Each field is described in the following table.

Table 50 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.

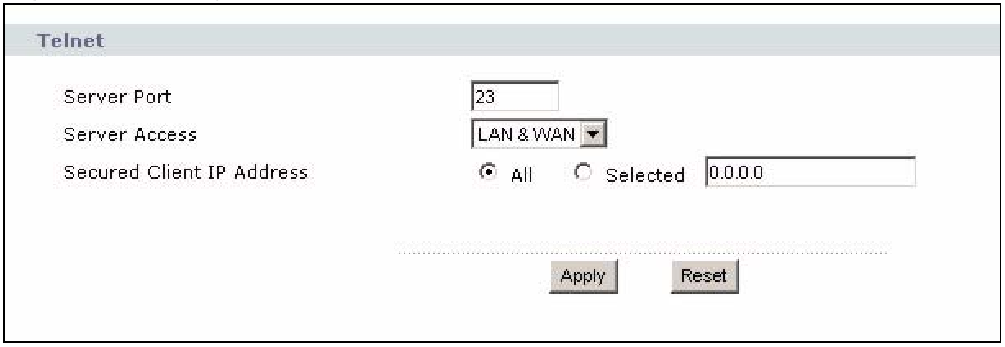
Table 50 Management > Remote MGMT > WWW

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

16.2.2 Telnet Screen

Use this screen to control Telnet access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > Telnet**.

Figure 86 Management > Remote MGMT > Telnet



Telnet

Server Port: 23

Server Access: LAN & WAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Each field is described in the following table.

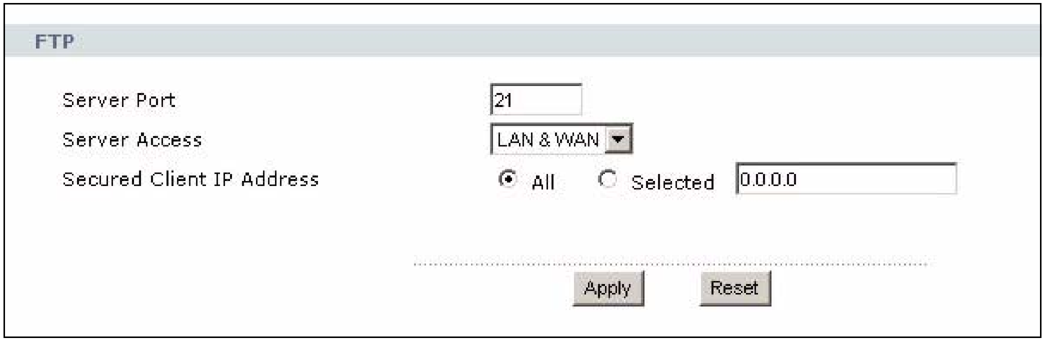
Table 51 Management > Remote MGMT > Telnet

LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its default value.

16.2.3 FTP Screen

Use this screen to control FTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > FTP**.

Figure 87 Management > Remote MGMT > FTP



FTP

Server Port: 21

Server Access: LAN & WAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Each field is described in the following table.

Table 52 Management > Remote MGMT > FTP

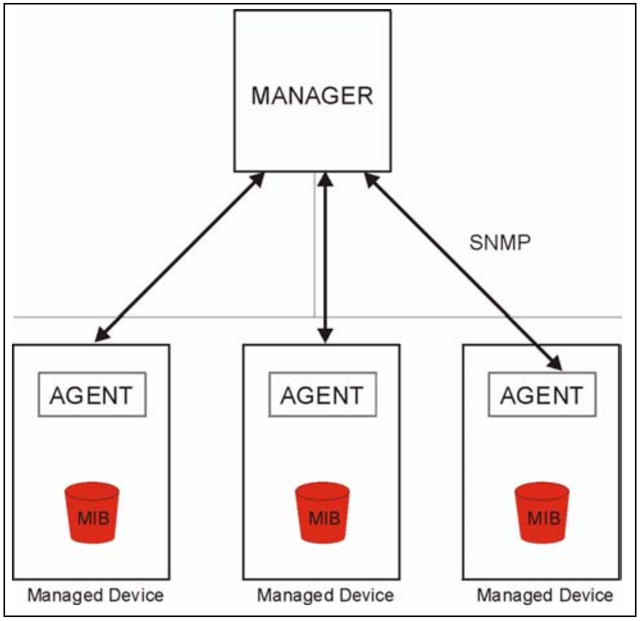
LABEL	DESCRIPTION
Server Port	Enter the port number this service can use to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

16.3 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 88 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

16.3.1 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

16.3.2 SNMP Traps

The ZyXEL Device will send traps to the SNMP manager when any one of the following events occurs:

Table 53 SNMP Traps

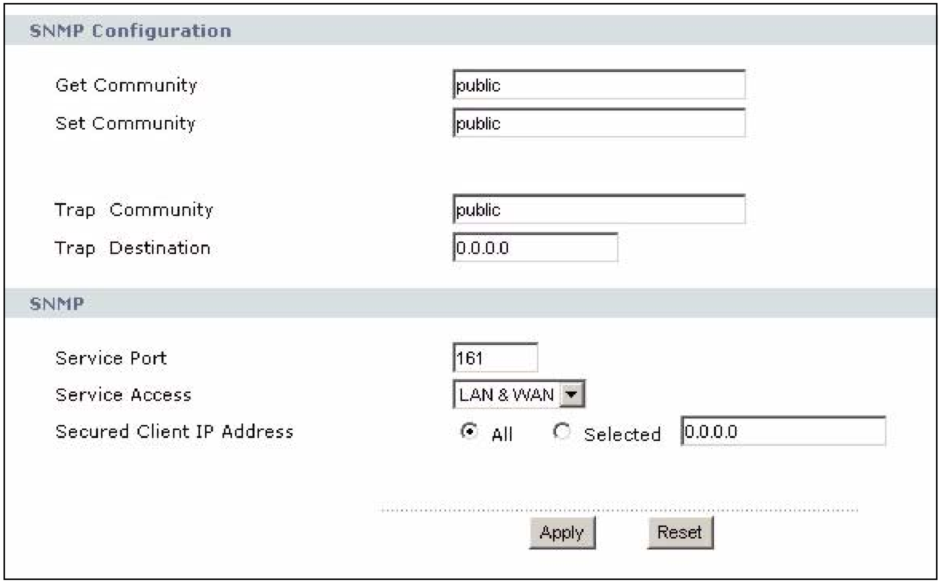
TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

16.3.3 Configuring SNMP

To change your ZyXEL Device’s SNMP settings, click **Advanced > Remote MGMT** > **SNMP**. The screen appears as shown.

Use this screen to control FTP access to your ZyXEL Device. To access this screen, click **Management > Remote MGMT > SNMP**.

Figure 89 Management > Remote MGMT > SNMP



SNMP Configuration

Get Community	public
Set Community	public
Trap Community	public
Trap Destination	0.0.0.0

SNMP

Service Port	161
Service Access	LAN & WAN
Secured Client IP Address	● All ○ Selected 0.0.0.0

The following table describes the labels in this screen.

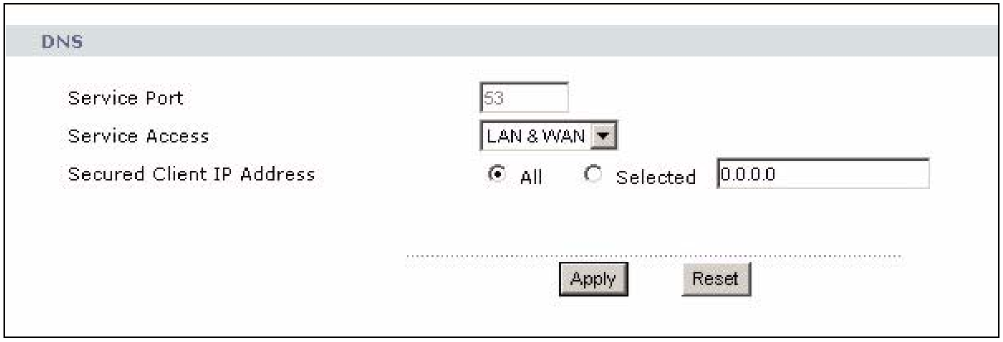
Table 54 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Trap Destination	Enter the IP address of the station to send your SNMP traps to.
SNMP	
Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Access Status	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this button to save your customized settings and exit this screen.
Reset	Click this button to set each field in this screen to its default value.

16.3.4 DNS Screen

Use this screen to control DNS access to your ZyXEL Device. To access this screen, click **Management** > **Remote MGMT** > **DNS**.

Figure 90 Management > Remote MGMT > DNS



DNS

Service Port: 53

Service Access: LAN & WAN

Secured Client IP Address: ● All ○ Selected 0.0.0.0

Each field is described in the following table.

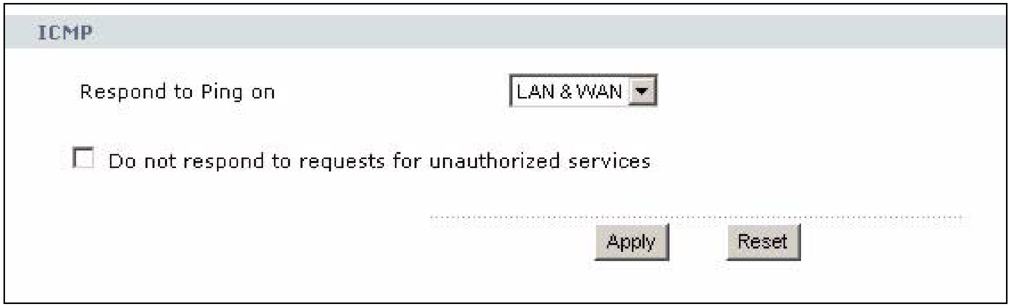
Table 55 Management > Remote MGMT > DNS

LABEL	DESCRIPTION
Server Port	This field is read-only. This field displays the port number this service uses to access the ZyXEL Device. The computer must use the same port number.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Select **Selected** to only allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Apply	Click this to save your changes.
Reset	Click this to set every field in this screen to its last-saved value.

16.3.5 Security Screen

Use this screen to control how your ZyXEL Device responds to other types of requests. To access this screen, click **Management > Remote MGMT > Security**.

Figure 91 Management > Remote MGMT > Security



ICMP

Respond to Ping on: LAN & WAN

□ Do not respond to requests for unauthorized services

Each field is described in the following table.

Table 56 Management > Remote MGMT > Security

LABEL	DESCRIPTION
Respond to Ping on	Select the interface(s) on which the ZyXEL Device should respond to incoming ping requests. **Disable** - the ZyXEL Device does not respond to any ping requests. **LAN** - the ZyXEL Device only responds to ping requests received from the LAN. **WAN** - the ZyXEL Device only responds to ping requests received from the WAN. **LAN & WAN** - the ZyXEL Device responds to ping requests received from the LAN or the WAN.
Do not respond to requests for unauthorized services	Select this to prevent outsiders from discovering your ZyXEL Device by sending requests to unsupported port numbers. If an outside user attempts to probe an unsupported port on your ZyXEL Device, an ICMP response packet is automatically returned. This allows the outside user to know the ZyXEL Device exists. Your ZyXEL Device supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your ZyXEL Device when unsupported ports are probed. If you clear this, your ZyXEL Device replies with an ICMP Port Unreachable packet for a port probe on unused UDP ports and with a TCP Reset packet for a port probe on unused TCP ports.
Apply	Click this to save your changes.
Cancel	Click this to set every field in this screen to its default value.

CHAPTER 17
UPnP

Use this screen to set up UPnP.

17.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

17.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

17.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See Chapter 9 on page 97 for further information about NAT.

17.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

17.1.4 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementors Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

The ZyXEL Device only sends UPnP multicasts to the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

17.2 UPnP Examples

17.2.1 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

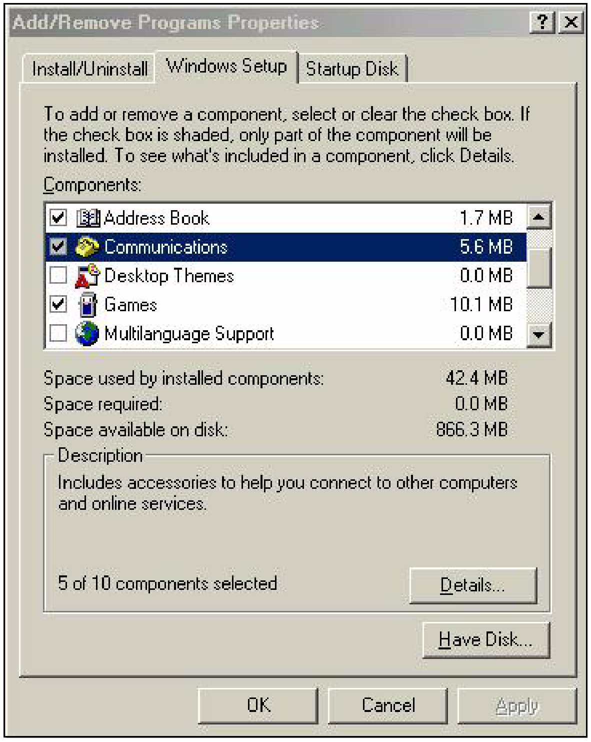
17.2.1.1 Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 92 Add/Remove Programs: Windows Setup: Communication



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
□	Desktop Themes	0.0 MB
☑	Games	10.1 MB
□	Multilanguage Support	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

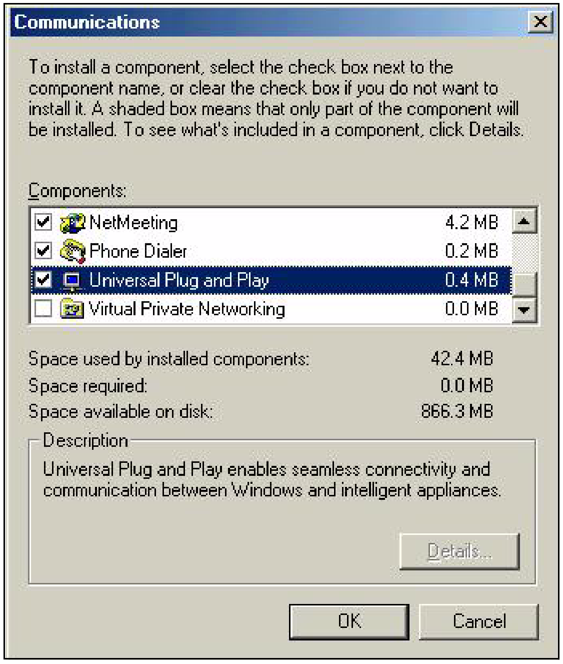
Description

Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 93 Add/Remove Programs: Windows Setup: Communication Components



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
□	Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description

Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

17.2.1.2 Installing UPnP in Windows XP

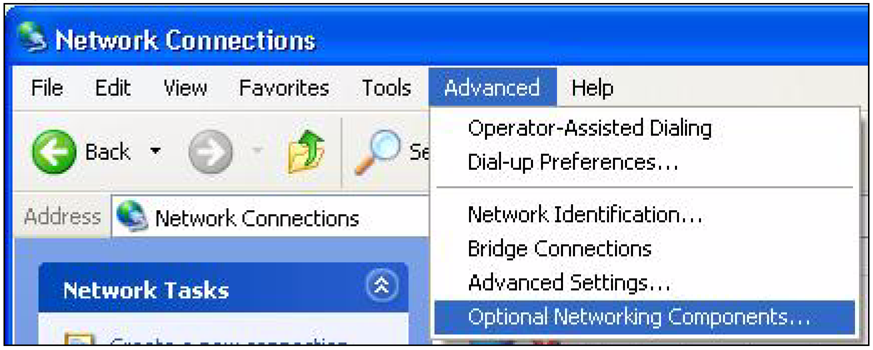
Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

2 Double-click **Network Connections**.

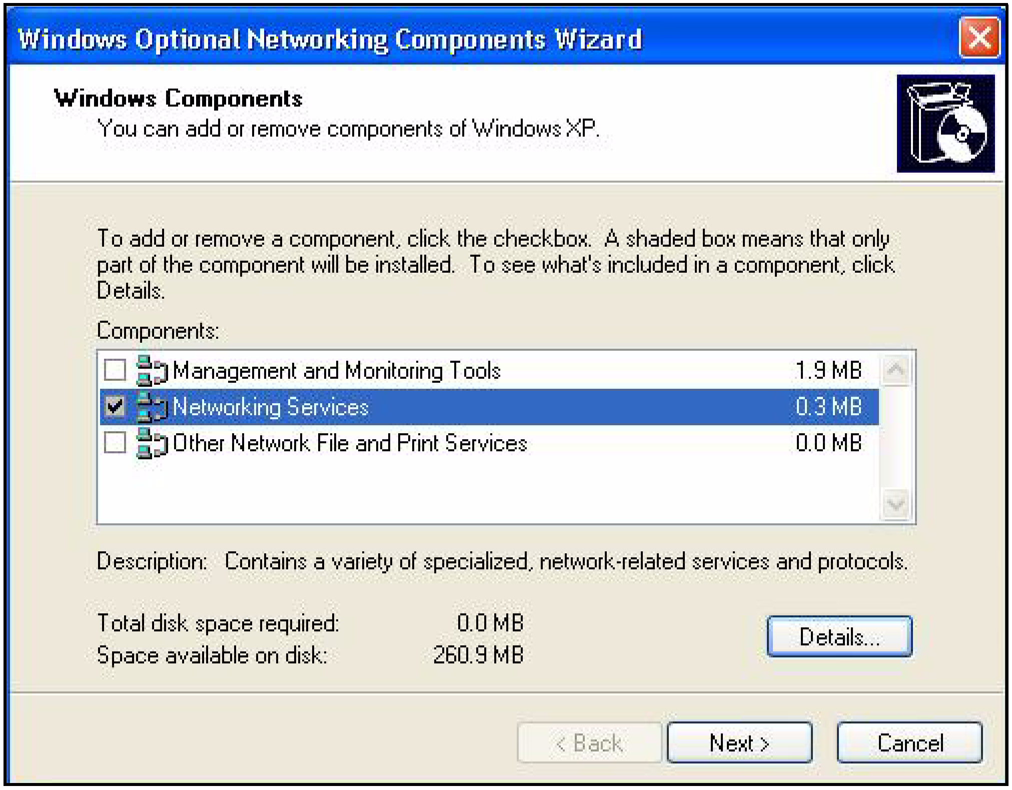
3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 94 Network Connections



4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 95 Windows Optional Networking Components Wizard



Windows Components

You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

□ Management and Monitoring Tools	1.9 MB
☑ Networking Services	0.3 MB
□ Other Network File and Print Services	0.0 MB

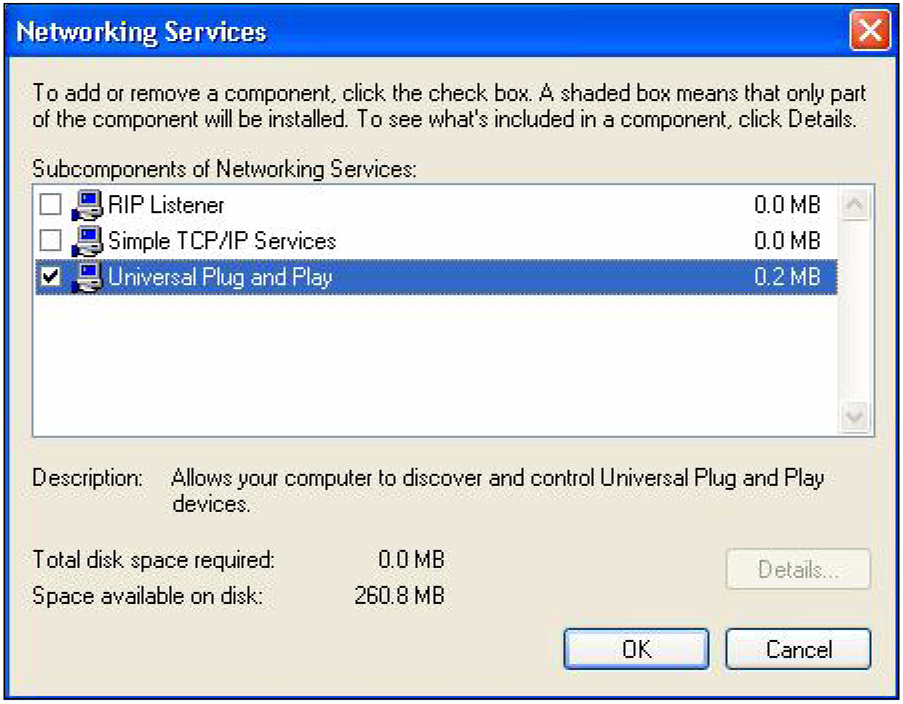
Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB

Space available on disk: 260.9 MB

5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 96 Networking Services



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

□ RIP Listener	0.0 MB
□ Simple TCP/IP Services	0.0 MB
☑ Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

17.2.2 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the ZyXEL Device.

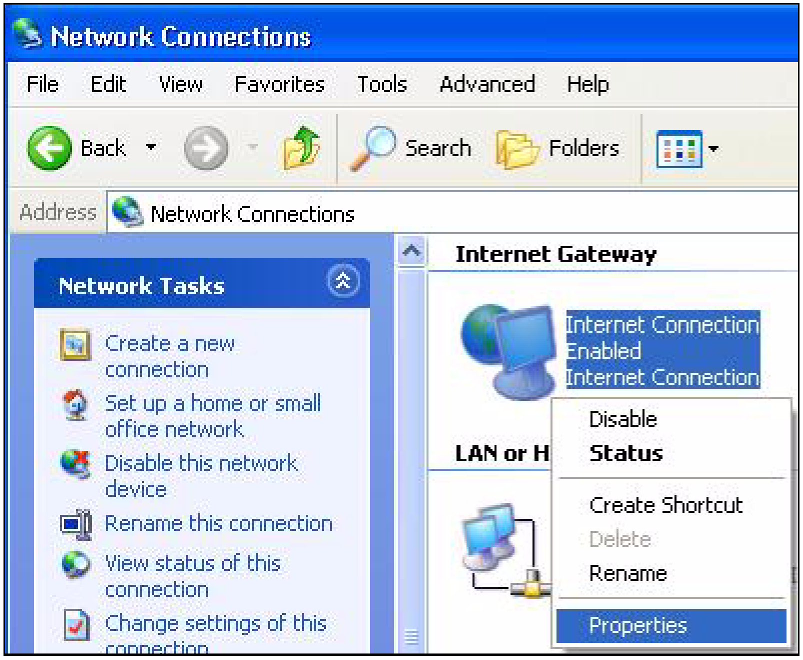
Make sure the computer is connected to a LAN port of the ZyXEL Device. Turn on your computer and the ZyXEL Device.

17.2.2.1 Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

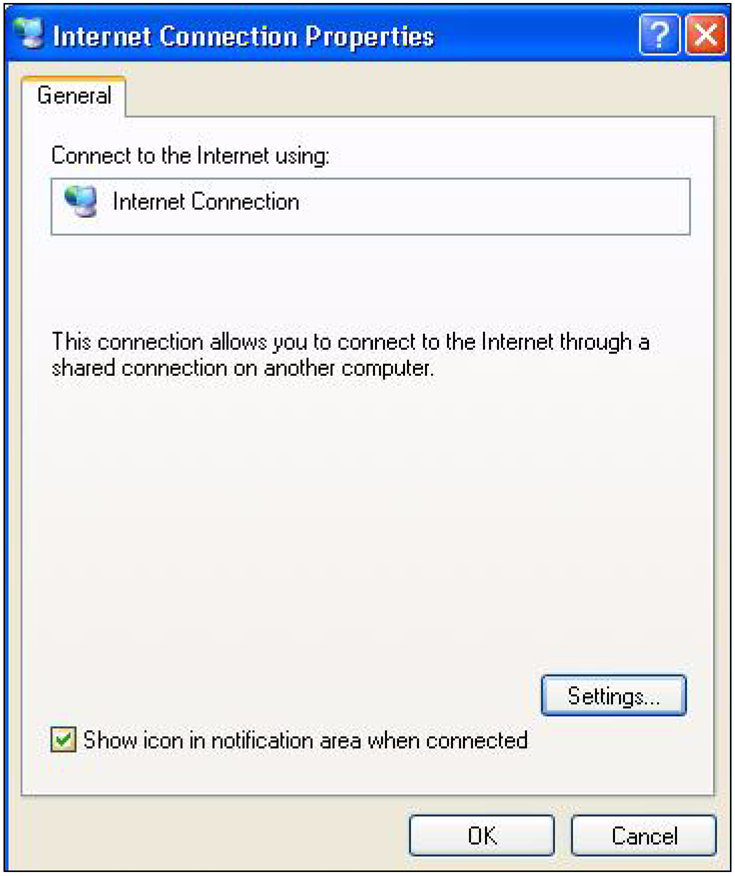
2 Right-click the icon and select **Properties**.

Figure 97 Network Connections



3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 98 Internet Connection Properties



Internet Connection Properties

Connect to the Internet using:

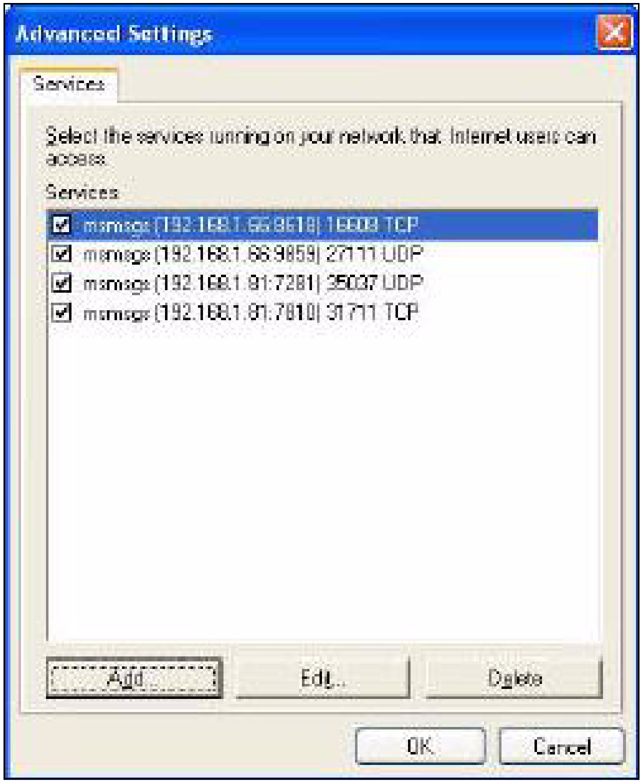
Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 99 Internet Connection Properties: Advanced Settings

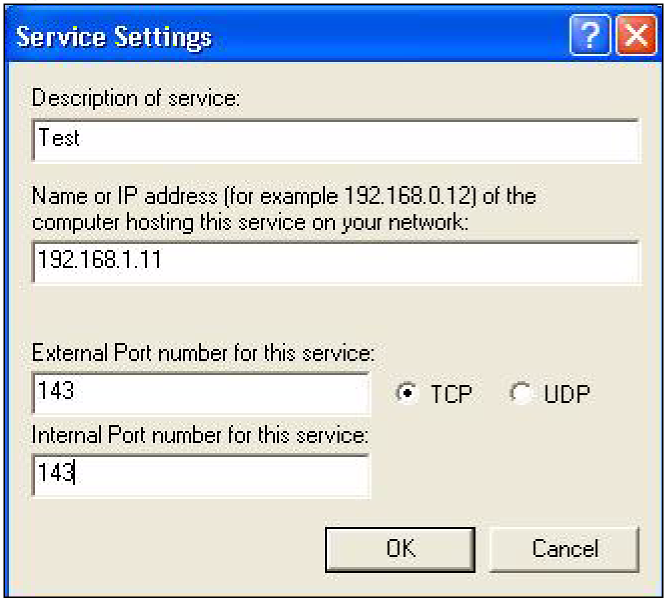


Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.91:7281) 35037 UDP
☑ msmsgs (192.168.1.91:7810) 31711 TCP

Figure 100 Internet Connection Properties: Advanced Settings: Add



Description of service: Test

Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network: 192.168.1.11

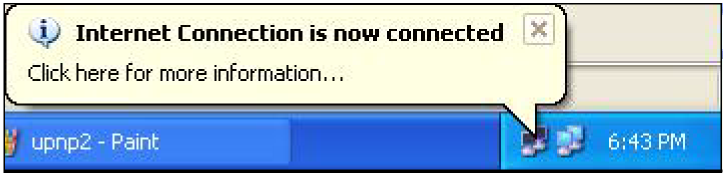
External Port number for this service: 143 ● TCP ○ UDP

Internal Port number for this service: 143

5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 101 System Tray Icon

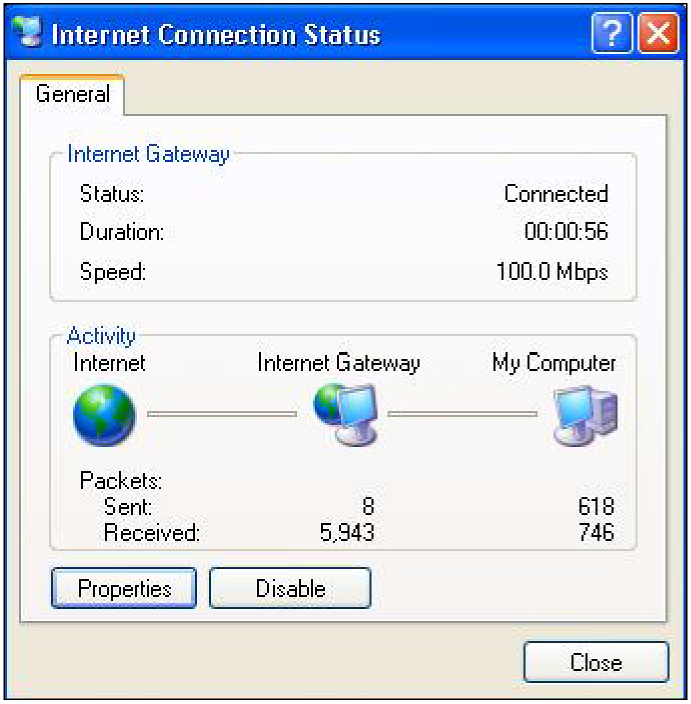


Internet Connection is now connected

Click here for more information...

7 Double-click on the icon to display your current Internet connection status.

Figure 102 Internet Connection Status



Internet Connection Status

Internet Gateway

Status: Connected

Duration: 00:00:56

Speed: 100.0 Mbps

Activity

	Internet Gateway	My Computer
Internet		
Packets:		
Sent:	8	618
Received:	5,943	746

17.2.2.2 Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the ZyXEL Device without finding out the IP address of the ZyXEL Device first. This becomes helpful if you do not know the IP address of the ZyXEL Device.

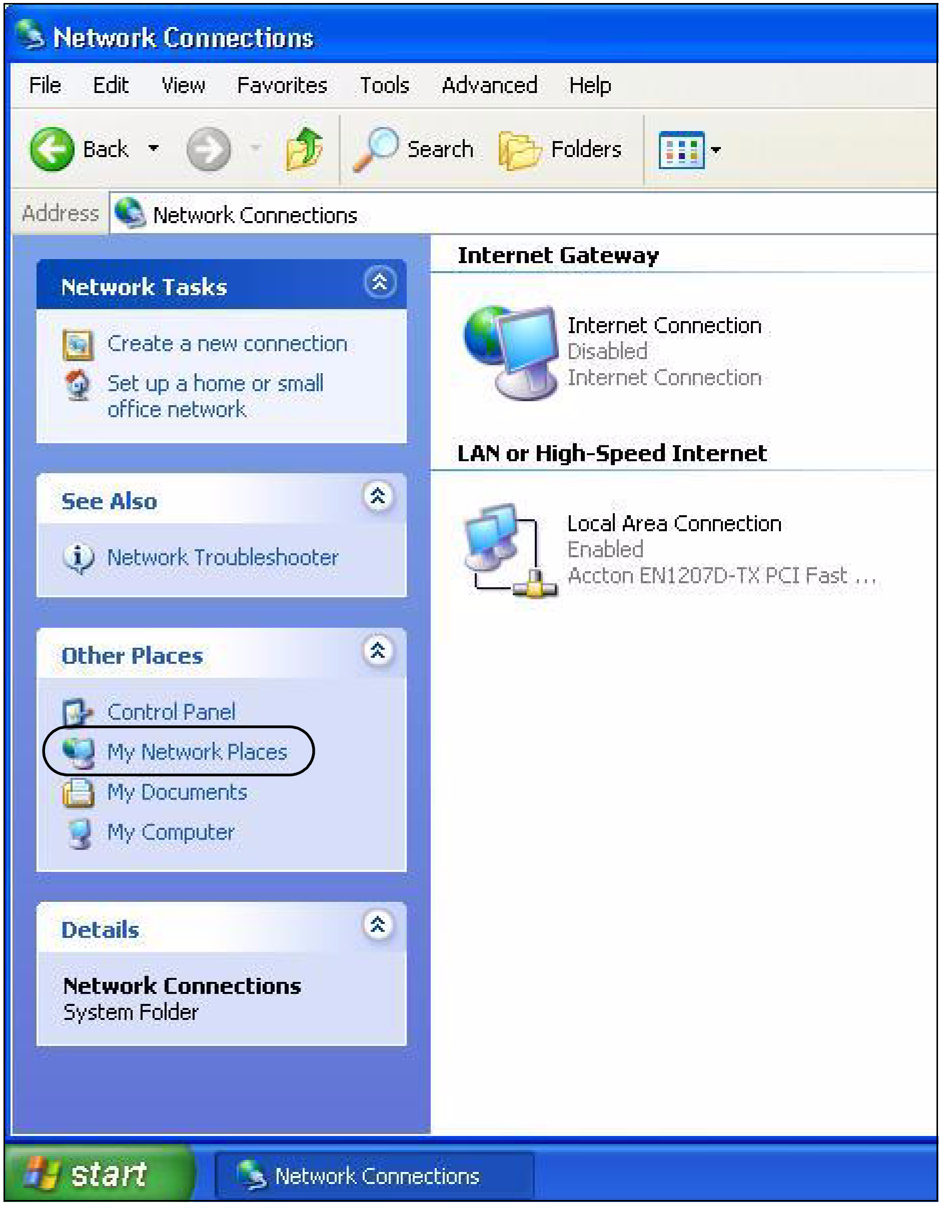
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

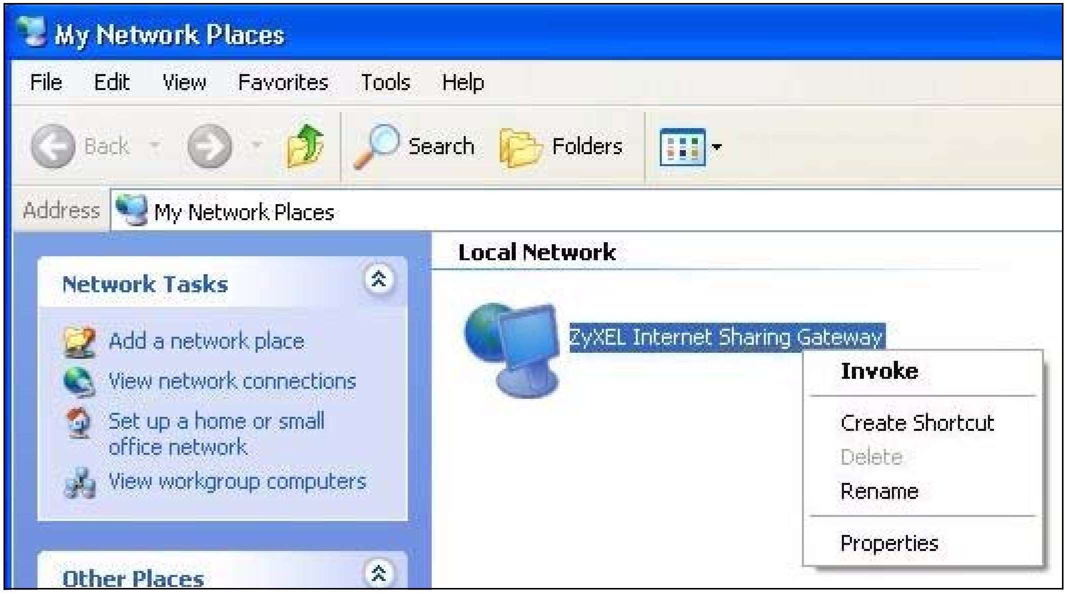
Figure 103 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

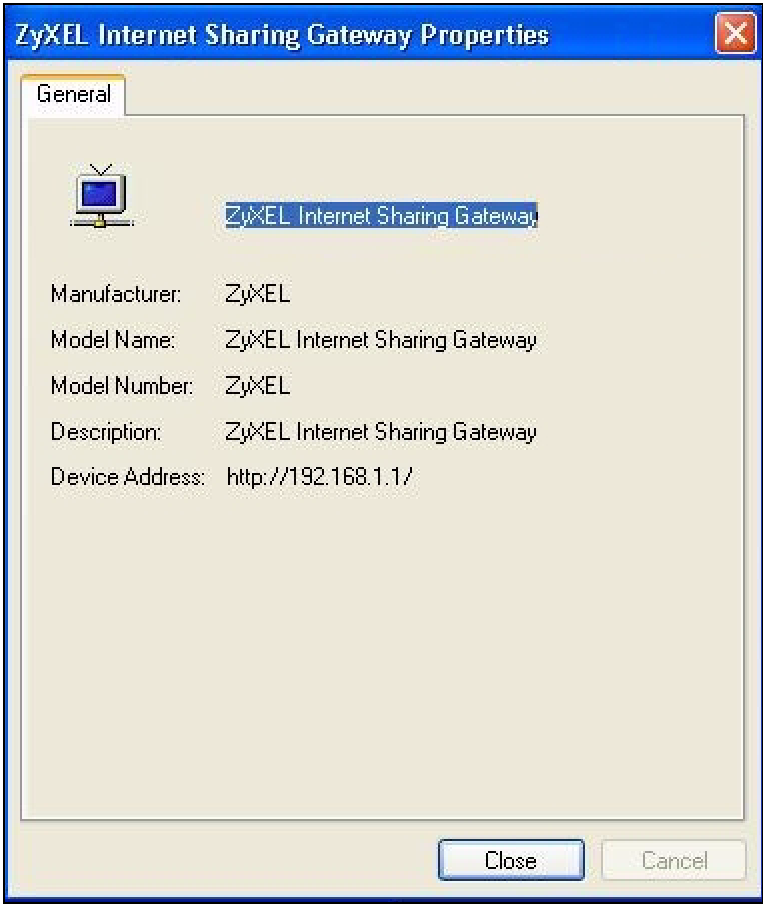
5 Right-click on the icon for your ZyXEL Device and select **Invoke**. The web configurator login screen displays.

Figure 104 Network Connections: My Network Places



6 Right-click on the icon for your ZyXEL Device and select **Properties**. A properties window displays with basic information about the ZyXEL Device.

Figure 105 Network Connections: My Network Places: Properties: Example



ZyXEL Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: ZyXEL

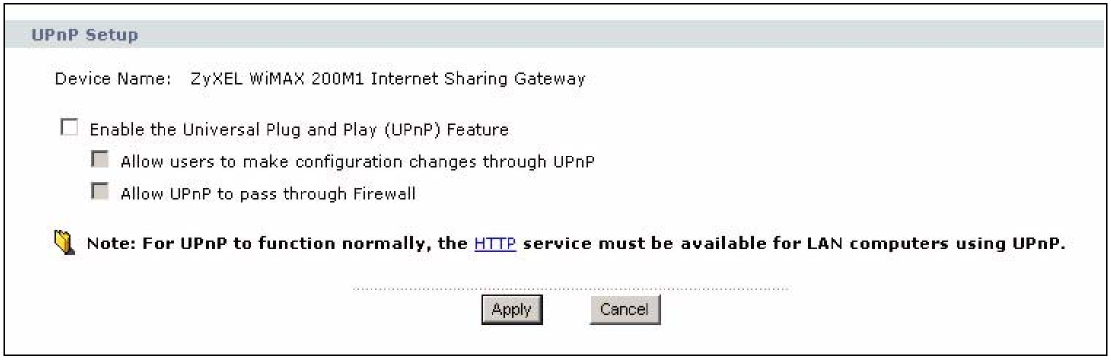
Description: ZyXEL Internet Sharing Gateway

Device Address: http://192.168.1.1/

17.3 UPnP Screen

Use this screen to set up UPnP in your ZyXEL Device. To access this screen, click **Management > UPnP**.

Figure 106 Management > UPnP



UPnP Setup

Device Name: ZyXEL WiMAX 200M1 Internet Sharing Gateway

☐ Enable the Universal Plug and Play (UPnP) Feature

☐ Allow users to make configuration changes through UPnP

☐ Allow UPnP to pass through Firewall

Note: For UPnP to function normally, the HTTP service must be available for LAN computers using UPnP.

Each field is described in the following table.

Table 57 Management > UPnP

LABEL	DESCRIPTION
Device Name	This field identifies your device in UPnP applications.
Enable the Universal Plug and Play (UPnP) Feature	Select this to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the ZyXEL Device's IP address. You still have to enter the password, however.
Allow users to make configuration changes through UPnP	Select this to allow UPnP-enabled applications to automatically configure the ZyXEL Device so that they can communicate through the ZyXEL Device. For example, using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this if you want the firewall to check UPnP application packets (for example, MSN packets).
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its default value.

CHAPTER 18
Logs

Use these screens to look at log entries and alerts and to configure the ZyXEL Device’s log and alert settings.

18.1 Logs Overview

For a list of log messages, see Section 18.3 on page 182.

18.1.1 Alerts

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts.

18.1.2 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

Table 58 Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the **Log Settings** screen. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/ Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example).

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 59 RFC-2408 ISAKMP Payload Types

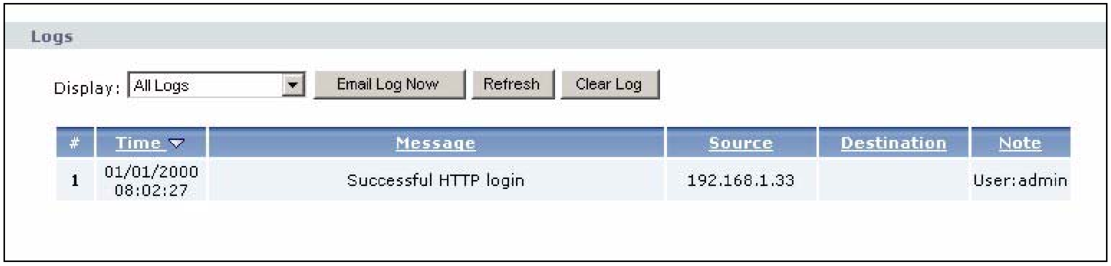
LOG DISPLAY	PAYLOAD TYPE
`SA`	Security Association
`PROP`	Proposal
`TRANS`	Transform
`KE`	Key Exchange
`ID`	Identification
`CER`	Certificate
`CER_REQ`	Certificate Request
`HASH`	Hash
`SIG`	Signature
`NONCE`	Nonce
`NOTFY`	Notification
`DEL`	Delete
`VID`	Vendor ID

18.2 Logs Screens

18.2.1 Log Viewer Screen

Use this screen to look at log entries and alerts. Alerts are written in red. To access this screen, click **Maintenance** > **Logs** > **View Log**.

Figure 107 Maintenance > Logs > View Log



#	Time	Message	Source	Destination	Note
1	01/01/2000 08:02:27	Successful HTTP login	192.168.1.33		User:admin

Click a column header to sort log entries in descending (later-to-earlier) order. Click again to sort in ascending order. The small triangle next to a column header indicates how the table is currently sorted (pointing downward is descending; pointing upward is ascending). Each field is described in the following table.

Table 60 Maintenance > Logs > View Log

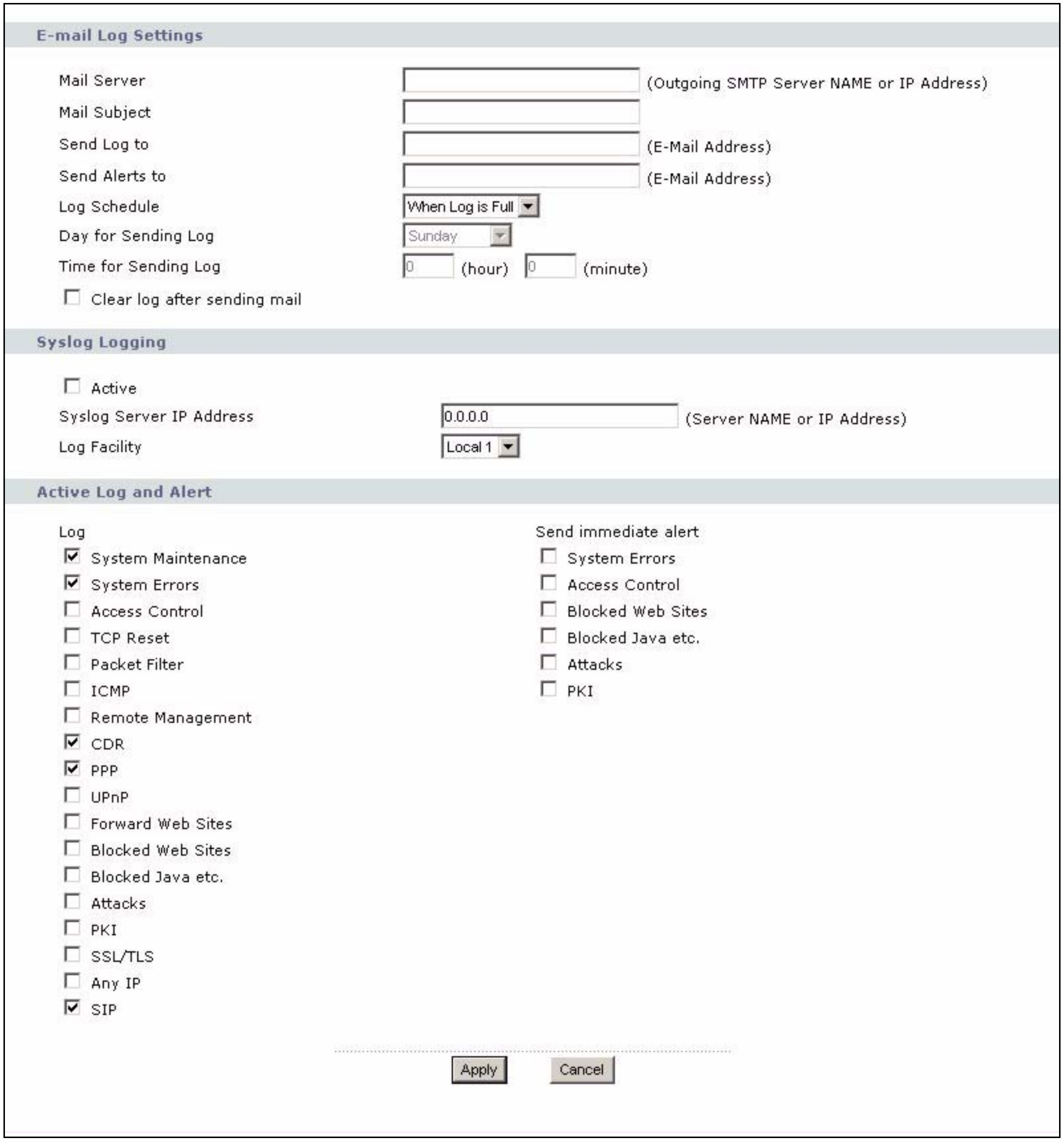
LABEL	DESCRIPTION
Display	Select a category whose log entries you want to view. To view all logs, select **All Logs**. The list of categories depends on what log categories are selected in the **Log Settings** page.
Email Log Now	Click this to send the log screen to the e-mail address specified in the **Log Settings** page.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the log entries, regardless of what is shown on the log screen.
#	This field is a sequential value, and it is not associated with a specific log entry.
Time	This field displays the time the log entry was recorded.
Message	This field displays the reason for the log entry. See Section 18.3 on page 182.
Source	This field displays the source IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Destination	This field lists the destination IP address and the port number of the incoming packet. In many cases, some or all of this information may not be available.
Note	This field displays additional information about the log entry.

18.2.2 Log Settings Screen

Use this screen to configure where the ZyXEL Device sends logs and alerts, the schedule for sending logs, and which logs and alerts are sent or recorded.

To access this screen, click **Maintenance > Logs > Log Settings**.

Figure 108 Maintenance > Logs > Log Settings



E-mail Log Settings

Mail Server (Outgoing SMTP Server NAME or IP Address)

Mail Subject

Send Log to (E-Mail Address)

Send Alerts to (E-Mail Address)

Log Schedule: When Log is Full

Day for Sending Log: Sunday

Time for Sending Log: 0 (hour) 0 (minute)

□ Clear log after sending mail

Syslog Logging

□ Active

Syslog Server IP Address: 0.0.0.0 (Server NAME or IP Address)

Log Facility: Local 1

Active Log and Alert

Log
- ☑ System Maintenance
- ☑ System Errors
- □ Access Control
- □ TCP Reset
- □ Packet Filter
- □ ICMP
- □ Remote Management
- ☑ CDR
- ☑ PPP
- □ UPnP
- □ Forward Web Sites
- □ Blocked Web Sites
- □ Blocked Java etc.
- □ Attacks
- □ PKI
- □ SSL/TLS
- □ Any IP
- ☑ SIP

Send immediate alert
- □ System Errors
- □ Access Control
- □ Blocked Web Sites
- □ Blocked Java etc.
- □ Attacks
- □ PKI

Each field is described in the following table.

Table 61 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
E-mail Log Settings	
Mail Server	Enter the server name or the IP address of the mail server the ZyXEL Device should use to e-mail logs and alerts. Leave this field blank if you do not want to send logs or alerts by e-mail.
Mail Subject	Enter the subject line used in e-mail messages the ZyXEL Device sends.

Table 61 Maintenance > Logs > Log Settings

LABEL	DESCRIPTION
Send Log to	Enter the e-mail address to which log entries are sent by e-mail. Leave this field blank if you do not want to send logs by e-mail.
Send Alerts to	Enter the e-mail address to which alerts are sent by e-mail. Leave this field blank if you do not want to send alerts by e-mail.
Log Schedule	Select the frequency with which the ZyXEL Device should send log messages by e-mail. • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Select which day of the week to send the logs.
Time for Sending Log	This field is only available when you select **Daily** or **Weekly** in the **Log Schedule** field. Enter the time of day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select this to clear all logs and alert messages after logs are sent by e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Select this to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that logs the selected categories of logs.
Log Facility	Select a location. The log facility allows you to log the messages in different files in the syslog server. See the documentation of your syslog for more details.
Active Log and Alert	
Log	Select the categories of logs that you want to record.
Send immediate alert	Select the categories of alerts that you want the ZyXEL Device to send immediately.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Cancel	Click this to set every field in this screen to its last-saved value.

18.3 Log Message Descriptions

The following tables provide descriptions of example log messages.

Table 62 System Error Logs

LOG MESSAGE	DESCRIPTION
`WAN connection is down.`	The WAN connection is down. You cannot access the network through this interface.
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Table 63 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The device has adjusted its time based on information from the time server.
`Time calibration failed`	The device failed to get information from the time server.
`WAN interface gets IP: %s`	The WAN interface got a new IP address from the DHCP or PPPoE server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`Successful WEB login`	Someone has logged on to the device's web configurator interface.
`WEB login failed`	Someone has failed to log on to the device's web configurator interface.
`TELNET Login Successfully`	Someone has logged on to the router via telnet.
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the device via ftp.
`FTP login failed`	Someone has failed to log on to the device via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Time initialized by Daytime Server`	The device got the time and date from the Daytime server.
`Time initialized by Time server`	The device got the time and date from the time server.
`Time initialized by NTP server`	The device got the time and date from the NTP server.
`Connect to Daytime server fail`	The device was not able to connect to the Daytime server.
`Connect to Time server fail`	The device was not able to connect to the Time server.
`Connect to NTP server fail`	The device was not able to connect to the NTP server.

Table 63 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Too large ICMP packet has been dropped`	The device dropped an ICMP packet that was too large.
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The device is saving configuration changes.

Table 64 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: [ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy’s setting.
`Firewall rule [NOT] match:[ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>, <rule:%d>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [TCP | UDP]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

Table 65 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.)
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.

Table 65 TCP Reset Logs (continued)

LOG MESSAGE	DESCRIPTION
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: `sys firewall tcprst`).

Table 66 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

For type and code details, see Table 74 on page 188.

Table 67 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.

Table 67 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 68 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE). "channel" or "ch" is the call channel ID.For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	The PPPoE or dial-up call is connected.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	The PPPoE or dial-up call was disconnected.

Table 69 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 70 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Table 71 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
`%s: Keyword blocking`	The content of a requested web page matched a user defined keyword.
`%s: Not in trusted web list`	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
`%s: Forbidden Web site`	The web site is in the forbidden web site list.
`%s: Contains ActiveX`	The web site contains ActiveX.
`%s: Contains Java applet`	The web site contains a Java applet.
`%s: Contains cookie`	The web site contains a cookie.
`%s: Proxy mode detected`	The router detected proxy mode in the packet.
`%s: Trusted Web site`	The web site is in a trusted domain.
`%s`	When the content filter is not on according to the time schedule.
`Waiting content filter server timeout`	The external content filtering server did not respond within the timeout period.
`DNS resolving failed`	The ZyXEL Device cannot get the IP address of the external content filtering via DNS query.
`Creating socket failed`	The ZyXEL Device cannot issue a query because TCP/IP socket creation failed, port:port number.
`Connecting to content filter server fail`	The connection to the external content filtering server failed.
`License key is invalid`	The external content filtering license key is invalid.

For type and code details, see Table 74 on page 188.

Table 72 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack.
`land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack.
`ip spoofing - WAN [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port.
`icmp echo : ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack.

Table 72 Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.

Table 73 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.

Table 73 Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

Table 74 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply

Table 74 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 75 SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account’s registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account’s registration from the SIP register server failed.

Table 76 RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

Table 77 FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number`	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
`VoIP Call Established Ph[Phone Port] -> Outgoing Call Number`	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call made from a phone connected to the listed phone port has terminated.

Table 78 FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
`VoIP Call Start from SIP[SIP Port Number]`	A VoIP phone call came to the ZyXEL Device from the listed SIP number.
`VoIP Call Established Ph[Phone Port] <- Outgoing Call Number`	A VoIP phone call was set up from the listed SIP number to the ZyXEL Device.
`VoIP Call End Phone[Phone Port]`	A VoIP phone call that came into the ZyXEL Device has terminated.

Table 79 Lifeline Logs

LOG MESSAGE	DESCRIPTION
`PSTN Call Start`	A PSTN call has been initiated.
`PSTN Call End`	A PSTN call has terminated.
`PSTN Call Established`	A PSTN call has been set up.

CHAPTER 19
Tools

Use these screens to upload new firmware, back up and restore the configuration, and restart the ZyXEL Device.

19.1 Tools Overview

19.1.1 ZyXEL Firmware

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "ZyXEL Device.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Note: Only use firmware for your ZyXEL Device's specific model. Refer to the label on the back of your ZyXEL Device.

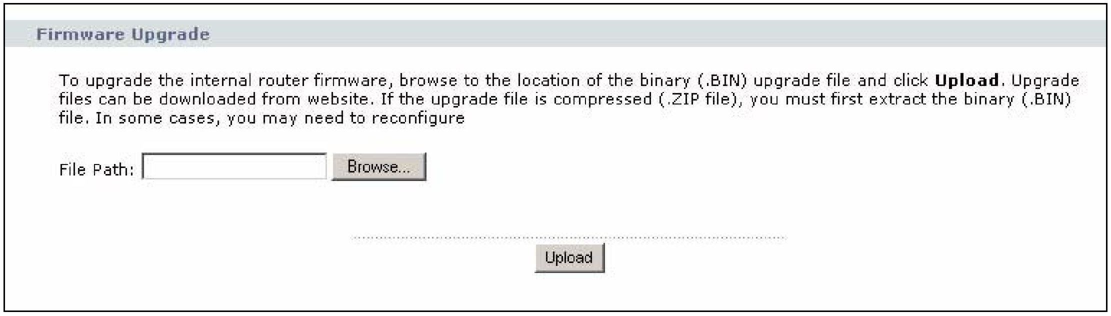
19.2 Tools Screens

19.2.1 Firmware Screen

Use this screen to upload new firmware to the ZyXEL Device. To access this screen, click **Maintenance** > **Tools** > **Firmware**.

Note: Only use firmware for your ZyXEL Device's specific model. Refer to the label on the bottom of your ZyXEL Device.

Figure 109 Maintenance > Tools > Firmware



Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **Upload**. Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN) file. In some cases, you may need to reconfigure

File Path:

Each field is described in the following table.

Table 80 Maintenance > Tools > Firmware

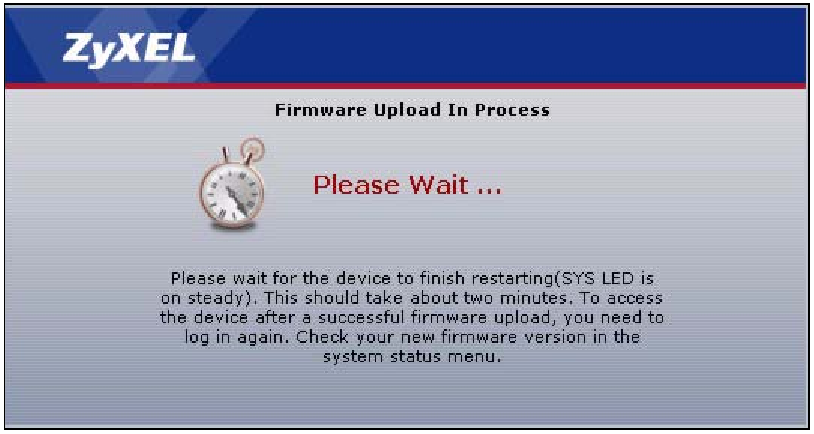
LABEL	DESCRIPTION
File Path	Enter the location of the .bin file you want to upload, or click **Browse...** to find it. You must decompress compressed (.zip) files before you can upload them.
Browse...	Click this to find the .bin file you want to upload.
Upload	Click this to begin uploading the selected file. This may take up to two minutes. See Section 19.2.2 on page 192 for more information about this process. **Note:** Do not turn off the device while firmware upload is in progress!

19.2.2 Firmware Upload Screens

Note: Do not turn off the device while firmware upload is in progress!

When the ZyXEL Device starts to upload firmware, the **Firmware Upload in Process** screen appears.

Figure 110 Firmware Upload In Process



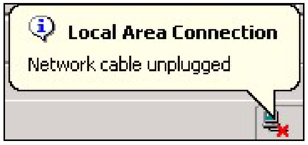
Firmware Upload In Process

Please Wait ...

Please wait for the device to finish restarting(SYS LED is on steady). This should take about two minutes. To access the device after a successful firmware upload, you need to log in again. Check your new firmware version in the system status menu.

The process usually takes about two minutes. The device automatically restarts in this time. This causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 111 Network Temporarily Disconnected



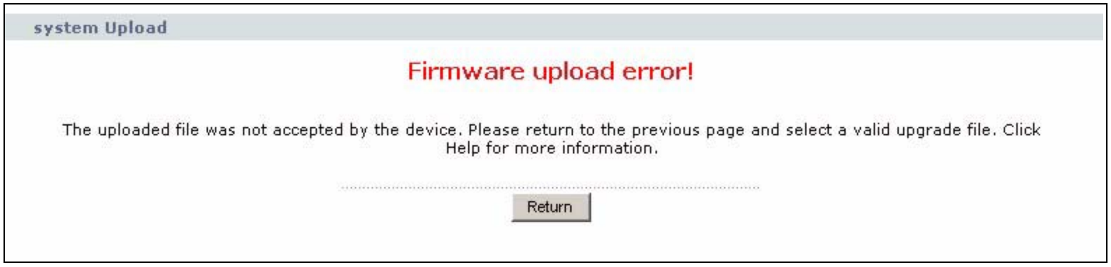
Local Area Connection

Network cable unplugged

After two minutes, log in again, and check your new firmware version in the **Status** screen. You might have to open a new browser to log in.

If the upload is not successful, the following screen appears.

Figure 112 Firmware Upload Error



system Upload

Firmware upload error!

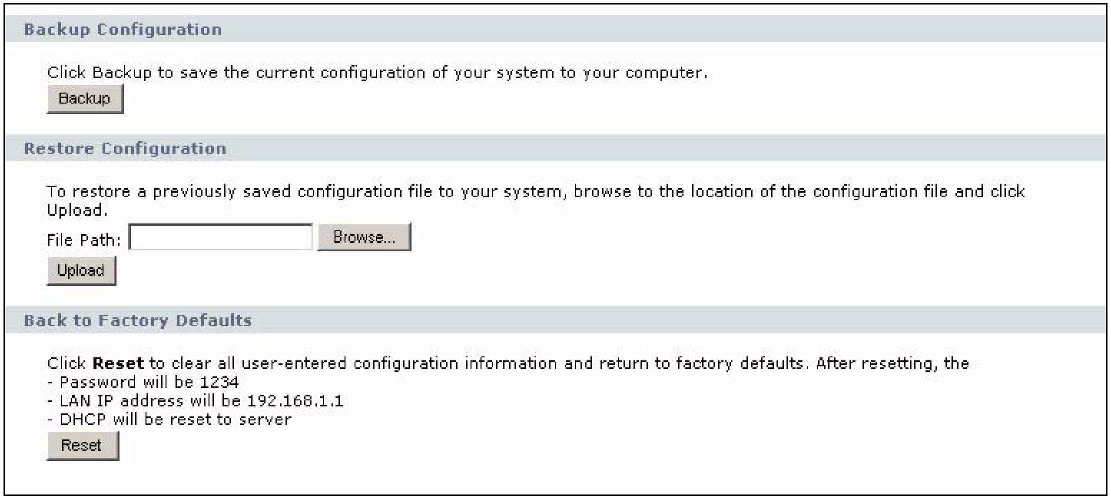
The uploaded file was not accepted by the device. Please return to the previous page and select a valid upgrade file. Click Help for more information.

Click **Return** to go back to the **Firmware** screen.

19.2.3 Configuration Screen

Use this screen to back up or restore the configuration of the ZyXEL Device. You can also use this screen to reset the ZyXEL Device to the factory default settings. To access this screen, click **Maintenance > Tools > Configuration**.

Figure 113 Maintenance > Tools > Configuration



Backup Configuration

Click Backup to save the current configuration of your system to your computer.

Restore Configuration

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.

File Path:

Back to Factory Defaults

Click **Reset** to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server

Each field is described in the following table.

Table 81 Maintenance > Tools > Configuration

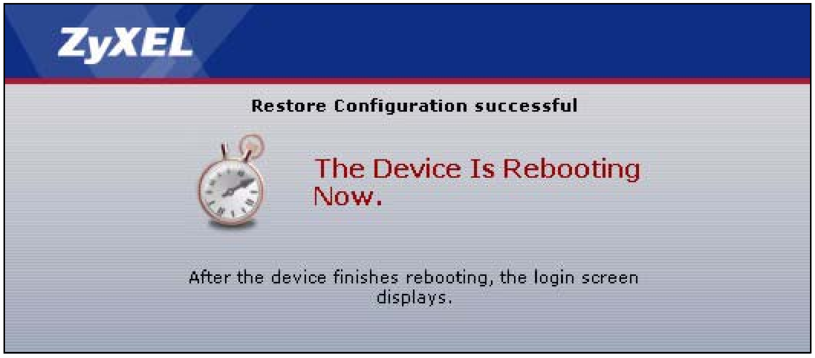
LABEL	DESCRIPTION
Backup Configuration	
Backup	Click this to save the ZyXEL Device's current configuration to a file on your computer. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file is useful if you need to return to your previous settings.
Restore Configuration	
File Path	Enter the location of the file you want to upload, or click **Browse...** to find it.
Browse	Click this to find the file you want to upload.
Upload	Click this to restore the selected configuration file. See Section 19.2.4 on page 194 for more information about this. **Note:** Do not turn off the device while configuration file upload is in progress.
Back to Factory Defaults	
Reset	Click this to clear all user-entered configuration information and return the ZyXEL Device to its factory defaults. There is no warning screen.

19.2.4 Restore Configuration Screens

Note: Do not turn off the device while configuration file upload is in progress.

When the ZyXEL Device has finished restoring the selected configuration file, the following screen appears.

Figure 114 Configuration Upload Successful



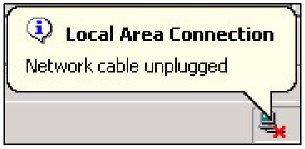
Restore Configuration successful

The Device Is Rebooting Now.

After the device finishes rebooting, the login screen displays.

The device now automatically restarts. This causes a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 115 Network Temporarily Disconnected



Local Area Connection

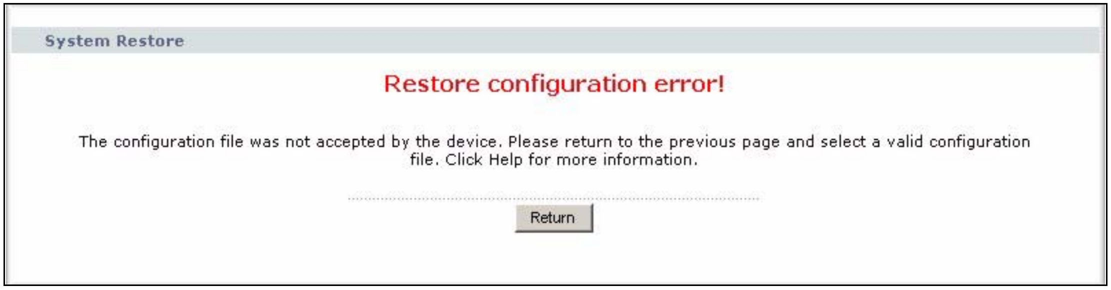
Network cable unplugged

If the ZyXEL Device's IP address is different in the configuration file you selected, you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See your Quick Start Guide or the appendices for details on how to set up your computer's IP address.

You might have to open a new browser to log in again.

If the upload was not successful, a **Configuration Upload Error** screen appears.

Figure 116 Configuration Upload Error



System Restore

Restore configuration error!

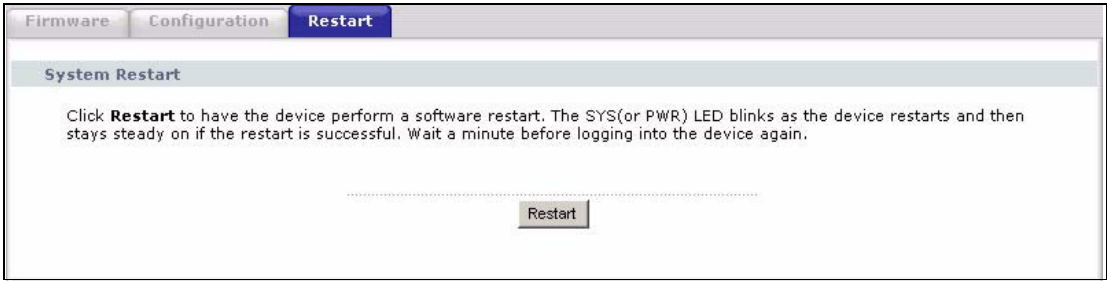
The configuration file was not accepted by the device. Please return to the previous page and select a valid configuration file. Click Help for more information.

Click **Return** to go back to the **Configuration** screen.

19.2.5 Restart Screen

Use this screen to reboot the ZyXEL Device without turning the power off. To access this screen, click **Maintenance** > **Tools** > **Restart**.

Figure 117 Maintenance > Tools > Restart

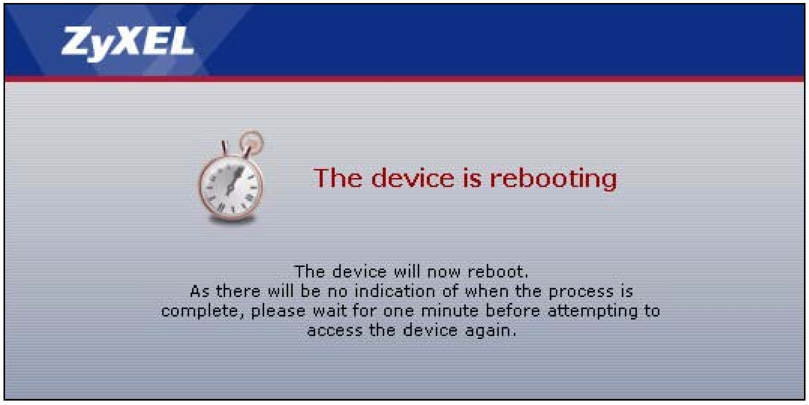


System Restart

Click **Restart** to have the device perform a software restart. The SYS(or PWR) LED blinks as the device restarts and then stays steady on if the restart is successful. Wait a minute before logging into the device again.

This does not affect the ZyXEL Device’s configuration. When you click **Restart**, the following screen appears.

Figure 118 Maintenance > Tools > Restart > In Progress



The device is rebooting

The device will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

Wait one minute for the device to finish restarting. Then, you can log in again.

CHAPTER 20 System

Use this screen to set up general system settings, change the system mode, change the password, configure the DDNS server settings, and set the current date and time.

20.1 System Features Overview

20.1.1 System Name

System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the ZyXEL Device **System Name**.

20.1.2 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the ZyXEL Device via DHCP.

20.1.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The ZyXEL Device can get the DNS server addresses in the following ways.

1 The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in the **SYSTEM General** screen.

2 If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **SYSTEM General** screen set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

20.1.4 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

20.1.5 Pre-defined NTP Time Servers List

The ZyXEL Device uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Note: The ZyXEL Device can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

Table 82 Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk

Table 82 Pre-defined NTP Time Servers

ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

20.1.6 Resetting the Time

The ZyXEL Device resets the time in the following instances:

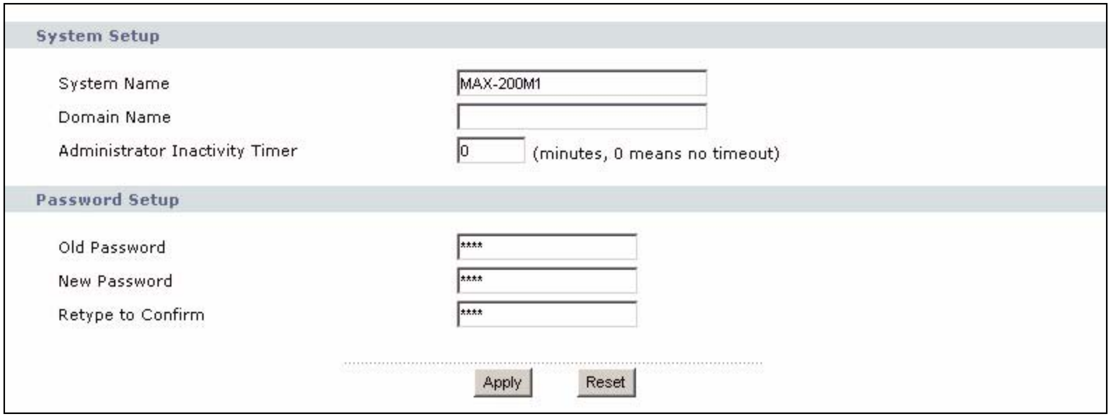
- When the ZyXEL Device starts up.
- When you click **Apply** in the Time Setting Screen.
- 24-hour intervals after starting.

20.2 System Screens

20.2.1 General System Screen

Use this screen to change the ZyXEL Device's mode, set up the ZyXEL Device's system name, domain name, idle timeout, and administrator password. To access this screen, click **Maintenance > System > General**.

Figure 119 Maintenance > System > General



System Setup

System Name: MAX-200M1

Domain Name:

Administrator Inactivity Timer: 0 (minutes, 0 means no timeout)

Password Setup

Old Password: ****

New Password: ****

Retype to Confirm: ****

Each field is described in the following table.

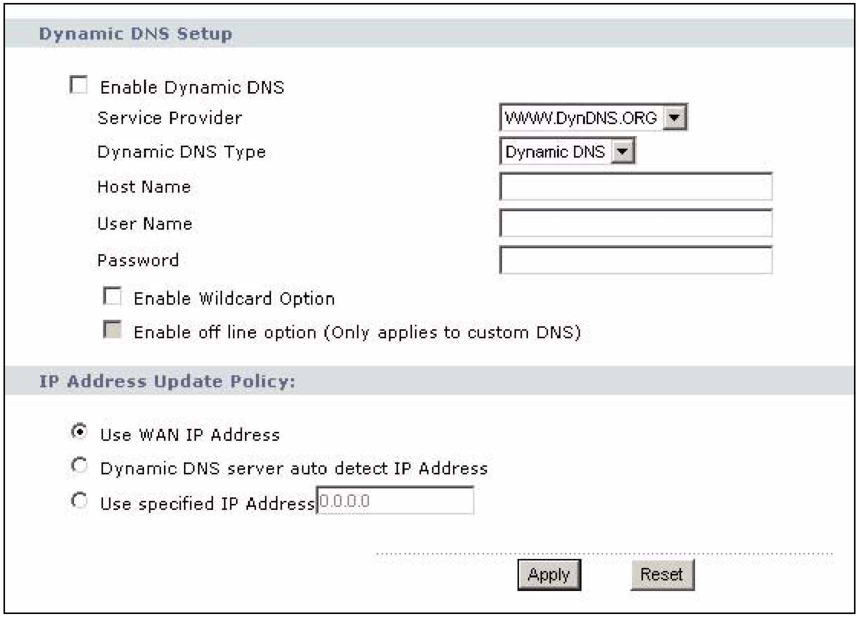
Table 83 Maintenance > System > General

LABEL	DESCRIPTION
System Setup	
System Name	Enter your computer's "Computer Name". This is for identification purposes, but some ISPs also check this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name entry that is propagated to DHCP clients on the LAN. If you leave this blank, the domain name obtained from the ISP is used. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted.
Administrator Inactivity Timer	Enter the number of minutes a management session can be left idle before the session times out. After it times out, you have to log in again. A value of "0" means a management session never times out, no matter how long it has been left idle. This is not recommended. Long idle timeouts may have security risks. The default is five minutes.
Password Setup	
Old Password	Enter the current password you use to access the ZyXEL Device.
New Password	Enter the new password for the ZyXEL Device. You can use up to 30 characters. As you type the password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Enter the new password again.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

20.2.2 Dynamic DNS Screen

Use this screen to set up the ZyXEL Device as a dynamic DNS client. To access this screen, click **Maintenance > System > Dynamic DNS**.

Figure 120 Maintenance > System > Dynamic DNS



Dynamic DNS Setup

☐ Enable Dynamic DNS

Service Provider	WWW.DynDNS.ORG
Dynamic DNS Type	Dynamic DNS
Host Name	
User Name	
Password	

☐ Enable Wildcard Option

☐ Enable off line option (Only applies to custom DNS)

IP Address Update Policy:

● Use WAN IP Address

○ Dynamic DNS server auto detect IP Address

○ Use specified IP Address 0.0.0.0

Each field is described in the following table.

Table 84 Maintenance > System > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS Setup	
Enable Dynamic DNS	Select this to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
Dynamic DNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Name	Enter the host name. You can specify up to two host names, separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select this to enable the DynDNS Wildcard feature.
Enable offline option	This field is available when **CustomDNS** is selected in the **DDNS Type** field. Select this if your Dynamic DNS service provider redirects traffic to a URL that you can specify while you are off line. Check with your Dynamic DNS service provider.
IP Address Update Policy	
Use WAN IP Address	Select this if you want the ZyXEL Device to update the domain name with the WAN port's IP address.

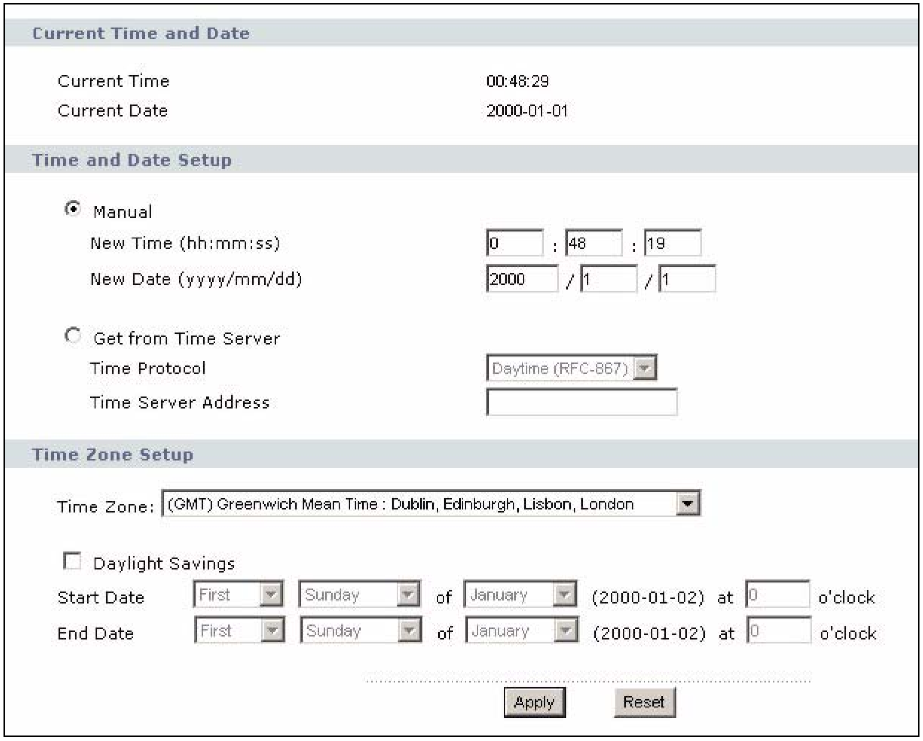
Table 84 Maintenance > System > Dynamic DNS

LABEL	DESCRIPTION
Dynamic DNS server auto detect IP address	Select this if you want the DDNS server to update the IP address of the host name(s) automatically. Select this option when there are one or more NAT routers between the ZyXEL Device and the DDNS server. **Note:** The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the ZyXEL Device and the DDNS server.
Use specified IP address	Select this if you want to use the specified IP address with the host name(s). Then, specify the IP address. Use this option if you have a static IP address.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its default value.

20.2.3 Time Setting Screen

Use this screen to set the date, time, and time zone in the ZyXEL Device. To access this screen, click **Maintenance > System > Time Setting**.

Figure 121 Maintenance > System > Time Setting



Current Time and Date

Current Time 00:48:29

Current Date 2000-01-01

Time and Date Setup

● Manual

New Time (hh:mm:ss) 0 : 48 : 19

New Date (yyyy/mm/dd) 2000 / 1 / 1

○ Get from Time Server

Time Protocol Daytime (RFC-867)

Time Server Address

Time Zone Setup

Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

□ Daylight Savings

Start Date First Sunday of January (2000-01-02) at 0 o'clock

End Date First Sunday of January (2000-01-02) at 0 o'clock

Each field is described in the following table.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Current Time and Date	This section displays the current date and time.
Time and Date Setup	
Manual	Select this if you want to specify the current date and time in the fields below.
New Time	Enter the new time in this field, and click **Apply**.
New Date	Enter the new date in this field, and click **Apply**.
Get from Time Server	Select this if you want to use a time server to update the current date and time in the ZyXEL Device.
Time Protocol	Select the time service protocol that your time server uses.Check with your ISP or network administrator, or use trial-and-error to find a protocol that works. **Daytime (RFC 867)** - This format is day/month/year/time zone. **Time (RFC 868)** - This format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC 1305)** - This format is similar to Time (RFC 868).
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Select the time zone at your location.

Table 85 Maintenance > System > Time Setting

LABEL	DESCRIPTION
Daylight Savings	Select this if your location uses daylight savings time. Daylight savings is a period from late spring to early fall when many places set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter which hour on which day of which week of which month daylight-savings time starts.
End Date	Enter which hour on the which day of which week of which month daylight-savings time ends.
Apply	Click this to save your changes and to apply them to the ZyXEL Device.
Reset	Click this to set every field in this screen to its last-saved value.

CHAPTER 21 Troubleshooting

This chapter covers potential problems and the corresponding remedies.

21.1 Problems Starting Up the ZyXEL Device

Table 86 Troubleshooting Starting Up Your Device

PROBLEM	CORRECTIVE ACTION
None of the lights turn on when I turn on the ZyXEL Device.	Make sure that the ZyXEL Device’s power adaptor is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure that the power source is turned on. Remove the power jack, then reinsert it. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

21.2 Problems with the LAN

Table 87 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The **LAN** light does not turn on.	Check your Ethernet cable connections (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer’s Ethernet Card is working properly.
I cannot access the ZyXEL Device from the LAN.	If **Any IP** is disabled, make sure that the IP address and the subnet mask of the ZyXEL Device and your computer(s) are on the same subnet.

21.3 Problems with the WAN

Table 88 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
I cannot connect to the Internet.	Check your connection. Look at the **LINK** and **SIGNAL** LEDs on the front of the ZyXEL Device. If the ZyXEL Device cannot detect a signal, follow the steps in Section 21.4 on page 206 to search for a wireless signal. Check your security settings. In the web configurator, go to the **Status** screen. Click **Profile** in the **WiMAX Information** box and make sure that you are using the correct security settings for your Internet account. Check your WiMAX settings. The ZyXEL Device may have been set to search the wrong frequencies for a wireless connection. In the web configurator, go to the **Status** screen. Click **Site Information** in the **WiMAX Information** box and ensure that the values are correct. If the values are incorrect, enter the correct frequency settings in the **Network > WAN > WiMAX Frequency** screen. If you are unsure of the correct values, contact your service provider. Check your IP address settings. You may be using IP address settings incompatible with your Internet account. If you are unsure of the correct settings, contact your service provider. See Appendix C on page 223 for information on how to set up your IP address.
The Internet connection disconnects.	Check your WiMAX link and signal strength using the **LINK** and **SIGNAL** LEDs on the device. See the following section if signal strength is poor or the ZyXEL Device has no link to a base station. Contact your ISP if the problem persists.

21.4 Problems with the Link Quality

Table 89 Troubleshooting Link Quality

PROBLEM	CORRECTIVE ACTION
Internet access is slow or intermittent.	The quality of the ZyXEL Device's wireless connection to the base station may be poor. Poor signal reception may be improved by moving the ZyXEL Device away from thick walls and other obstructions, or to a higher floor in your building. There may be radio interference caused by nearby electrical devices such as microwave ovens and radio transmitters. Move the ZyXEL Device away or switch the other devices off. Weather conditions may also affect signal quality.
	As well as having an external antenna connector, the ZyXEL Device is equipped with an internal directional antenna. If you know the location of the base station, orient the front of the ZyXEL Device (the side with the LEDs) towards the base station. If you do not know the location of the base station, experiment by moving the ZyXEL Device while observing the **SIGNAL** LEDs for an increase in received signal strength.

21.5 Problems Accessing the ZyXEL Device

Table 90 Troubleshooting Accessing Your Device

PROBLEM	CORRECTIVE ACTION
I cannot access the ZyXEL Device.	The default password is "1234". The **Password** field is case-sensitive. Make sure that you enter the correct password, using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not a telnet session running. Use the ZyXEL Device's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the ZyXEL Device's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. Your computer's and the ZyXEL Device's IP addresses must be on the same subnet for LAN access. If you changed the ZyXEL Device's LAN IP address, then enter the new one as the URL. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.
	You may also need to clear your Internet browser's cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.
I cannot remotely manage the ZyXEL Device from the LAN or WAN.	Refer to Chapter 21 on page 205 for scenarios when remote management may not be possible.
	Use the ZyXEL Device's WAN IP address when configuring from the WAN. Use the ZyXEL Device's LAN IP address when configuring from the LAN.

21.5.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

21.5.1.1 Internet Explorer Pop-up Blockers

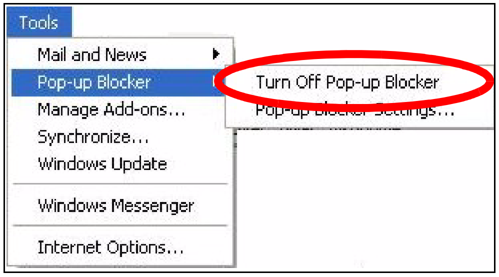
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

21.5.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 122 Pop-up Blocker

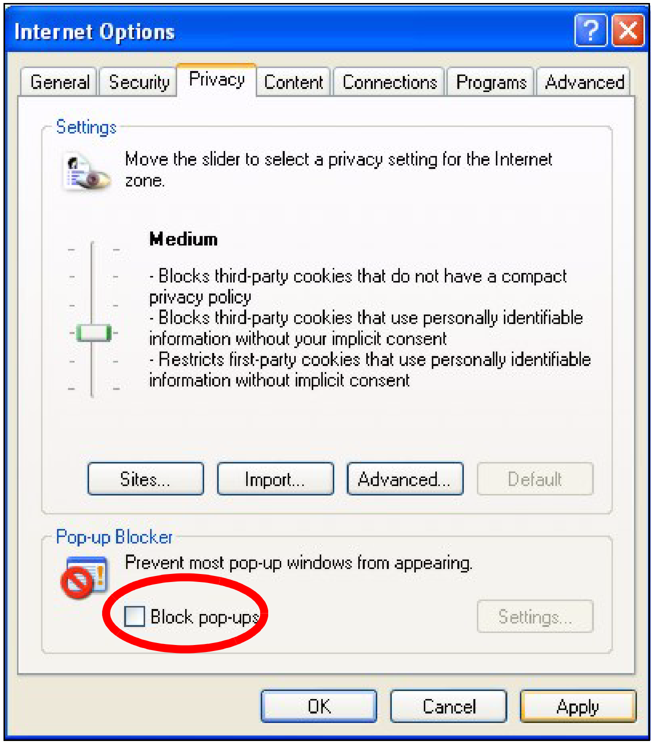


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 123 Internet Options



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

□ Block pop-ups

3 Click **Apply** to save this setting.

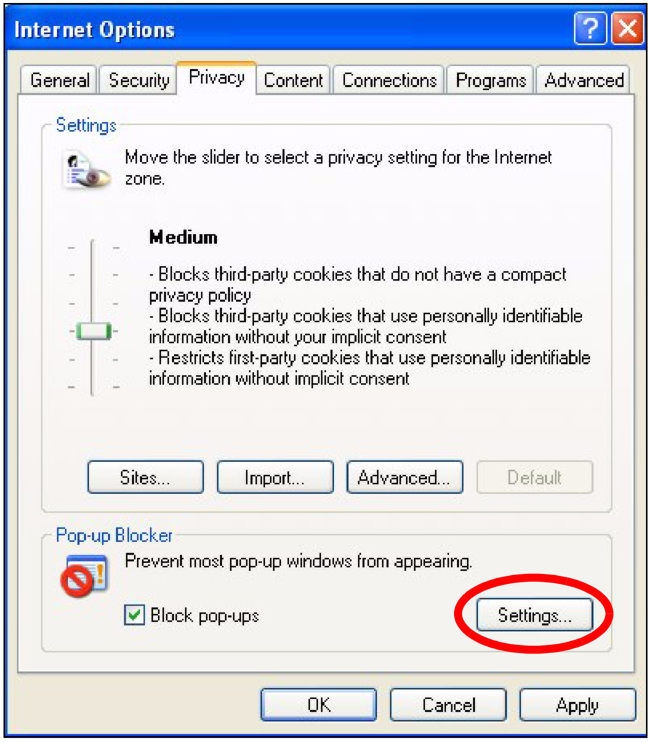
21.5.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 124 Internet Options



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

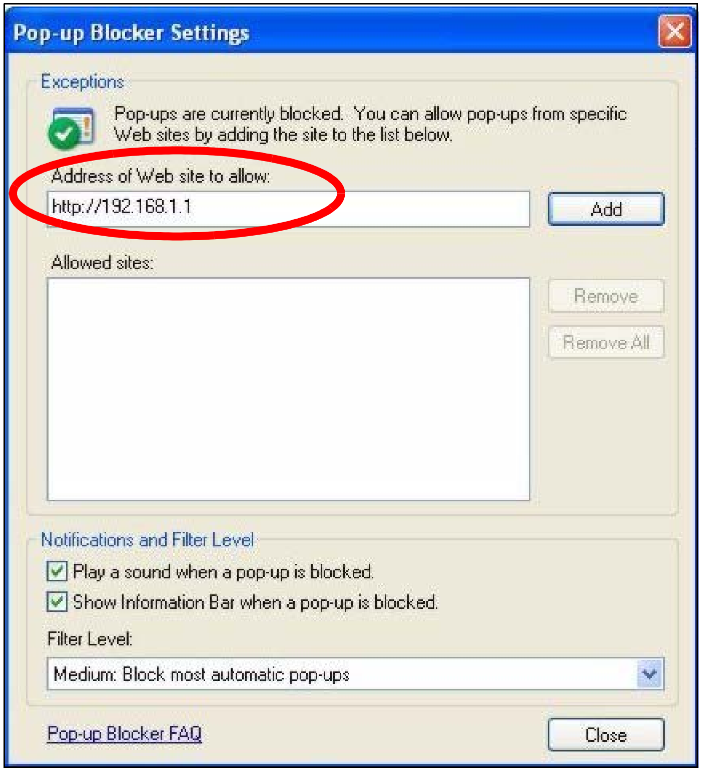
Prevent most pop-up windows from appearing.

☑ Block pop-ups

3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 125 Pop-up Blocker Settings



Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

5 Click **Close** to return to the **Privacy** screen.

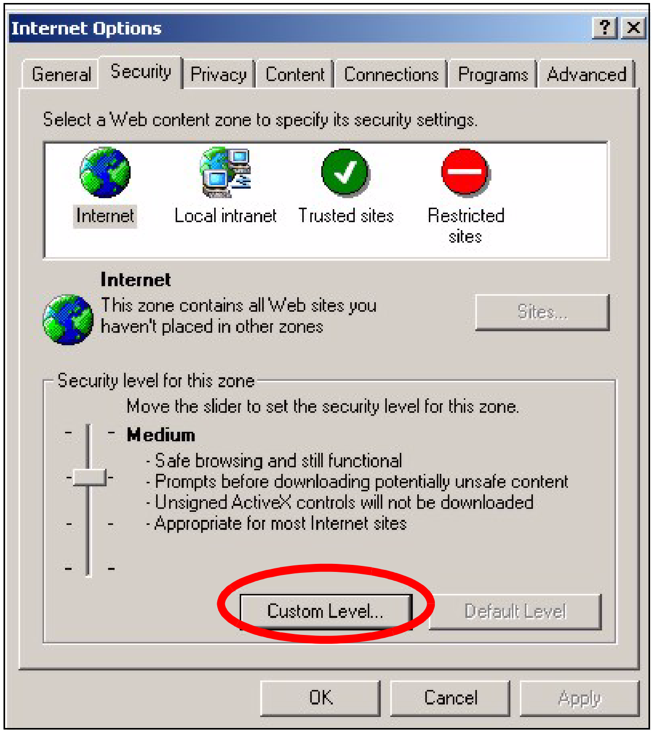
6 Click **Apply** to save this setting.

21.5.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 126 Internet Options



Select a Web content zone to specify its security settings.

Internet
This zone contains all Web sites you haven't placed in other zones

Move the slider to set the security level for this zone.

Medium
- Safe browsing and still functional
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded
- Appropriate for most Internet sites

2 Click the **Custom Level...** button.

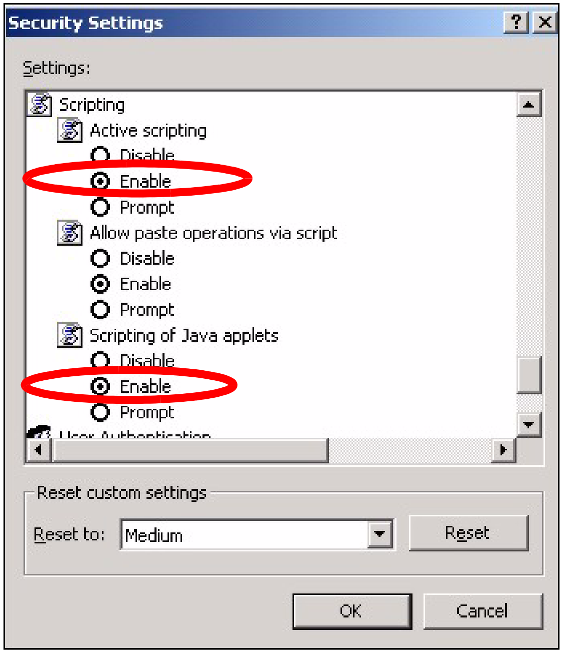
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 127 Security Settings - Java Scripting



Security Settings

Settings:

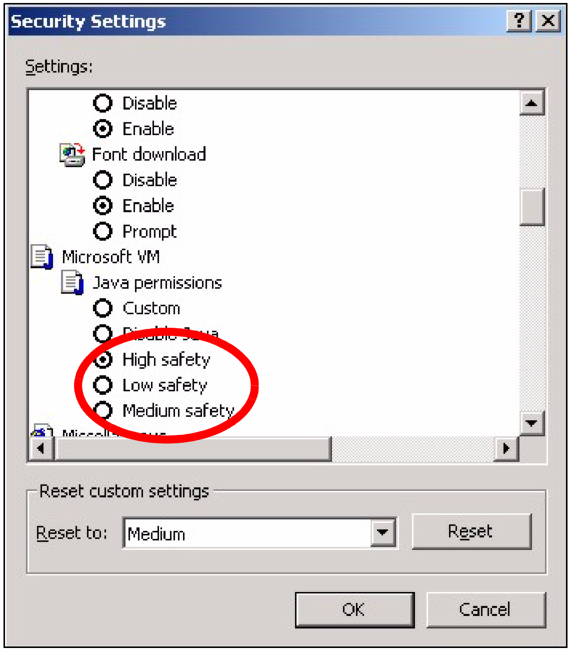
Scripting
- Active scripting
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Allow paste operations via script
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Scripting of Java applets
  - ○ Disable
  - ● Enable
  - ○ Prompt

User Authentication

21.5.1.3 Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

Figure 128 Security Settings - Java



Security Settings

Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt

Microsoft VM
- Java permissions
  - ○ Custom
  - ○ Disable Java
  - ● High safety
  - ○ Low safety
  - ○ Medium safety

Miscellaneous

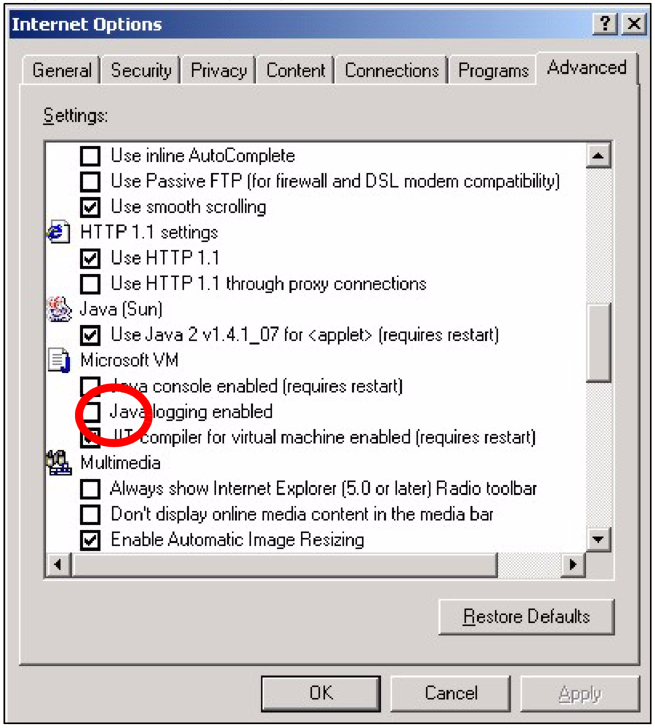
21.5.1.3.1 JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 129 Java (Sun)



☐ Use inline AutoComplete
☐ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
☐ Java console enabled (requires restart)
☐ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
☐ Always show Internet Explorer (5.0 or later) Radio toolbar
☐ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

21.6 Telephone Problems

Table 91 Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
The telephone port won't work or the telephone lacks a dial tone.	Check the telephone connections and telephone wire. Make sure you have the **VoIP SIP Settings** screen properly configured.
I can access the Internet, but cannot make VoIP calls.	Make sure you have the **VoIP SIP Settings** screen properly configured. The **VoIP** LED should come on. Make sure that your telephone is connected to the **LINE** port. You can also check the VoIP status in the **Status** screen. If the VoIP settings are correct, use speed dial to make peer-to-peer calls. If you cannot make a call using speed dial, there may be something wrong with the SIP server. Contact your VoIP service provider.

21.7 Problems With Multiple SIP Accounts

You can set up two SIP accounts on your ZyXEL Device. By default your ZyXEL Device uses SIP account 1 for outgoing calls, and it uses SIP accounts 1 and 2 for incoming calls. With this setting, you always use SIP account 1 for your outgoing calls and you cannot distinguish which SIP account the calls are coming in through. If you want to control the use of different dialing plans for accounting purposes or other reasons, you need to configure your phone port in order to control which SIP account you are using when placing or receiving calls.

APPENDIX A

Product Specifications

Table 92 Product Specifications

PHYSICAL AND ENVIRONMENTAL	
Product Name	ZyXEL MAX-200M1 Series IEEE 802.16e Simple Indoor CPE
Interface	Auto-negotiating, auto-MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
Standards	IEEE 802.16e-2005
Antenna	Built-in patch antenna: 6dBi, 70° azimuth, 30° elevation SMA antenna connector, equipped by default with 2dBi omni antenna, 60°
Operating Temperature	0 ~ 45 degrees Centigrade
Storage Temperature	-25 ~ 55 degrees Centigrade
Operating Humidity	10% ~ 90% (non-condensing)
Storage Humidity	10% ~ 100%
Power Supply	18 V DC
Power consumption	Worst-case-scenario 10W, peak 15W
Weight	389g
Dimensions	120 x 160 x 50mm
RADIO SPECIFICATIONS	
Media Access Protocol	IEEE 802.16e
WiMAX Bandwidth	MAX-200M1: 2.5 - 2.7 GHz MAX-210M1: 3.4 ~ 3.6 GHz MAX-230M1: 2.3 ~ 2.4 GHz
Data Rate	Downlink: Maximum 5 Mbps Uplink: Maximum 2 Mbps
Modulation	QPSK (uplink and downlink) 16-QAM (uplink and downlink) 64-QAM (downlink only)
Output Power	27dBm (+/- 1dB)
Duplex mode	Time Division Duplex (TDD)
SOFTWARE SPECIFICATIONS	
Security	PKMv2 EAP CCMP, 128-bit AES

Table 93 Physical Features

FEATURE	DESCRIPTION
Auto-crossover 10/100 Mbps Ethernet Interface	This interface automatically adjusts to either a crossover or straight-through Ethernet cable.
External Antenna	The ZyXEL Device is equipped with an attached antenna to provide a clear radio connection with the WiMAX base station.
Telephone Port	Connect an analog telephone to the ZyXEL Device's **LINE** port (RJ-11 connector) to take advantage of its Voice over IP (VoIP) features.
Reset Button	The reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

Table 94 Non-Physical Features

FEATURE	DESCRIPTION
High Speed Wireless Internet Access	The ZyXEL Device is ideal for high-speed wireless Internet browsing. WiMAX (Worldwide Interoperability for Microwave Access) is a wireless networking standard providing high-bandwidth, wide-range secured wireless service. The ZyXEL Device is a WiMAX mobile station (MS) compatible with the IEEE 802.16e standard.
Firewall	The ZyXEL Device is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The ZyXEL Device's firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.
Content Filtering	The ZyXEL Device can block access to web sites containing specified keywords. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.
Any IP	The Any IP feature allows a computer to access the Internet and the ZyXEL Device without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the ZyXEL Device are not in the same subnet.
Auto Provisioning	Your Internet service provider can automatically update your device's configuration via an auto-provisioning server.
Auto Firmware Upgrade	Your device gives you the option to upgrade to a newer firmware version if it finds one during auto-provisioning. Your VoIP service provider must have an auto-provisioning server and a server set up with firmware in order for this feature to work.
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).
Universal Plug and Play (UPnP)	Your device and other UPnP enabled devices can use the standard TCP/IP protocol to dynamically join a network, obtain an IP address and convey their capabilities to each other.

Table 94 Non-Physical Features

FEATURE	DESCRIPTION
Dynamic DNS Support	With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.
DHCP	DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Your device has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. Your device can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.
Multiple PVC (Permanent Virtual Circuits) Support	Your device supports up to 8 Permanent Virtual Circuits (PVCs).
IP Alias	IP alias allows you to partition a physical network into logical networks over the same Ethernet interface. Your device supports three logical LAN interfaces via its single physical Ethernet interface with the your device itself as the gateway for each LAN network.
IP Policy Routing (IPPR)	Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.
REN	A Ringer Equivalence Number (REN) is used to determine the number of devices (like telephones or fax machines) that may be connected to the telephone line. Your device has a REN of three, so it can support three devices per telephone port.
Multiple SIP Accounts	You can configure multiple voice (SIP) accounts.
SIP ALG	Your device is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind it (such as a SIP-based VoIP software application on a computer).
Dynamic Jitter Buffer	The built-in adaptive buffer helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.
Voice Activity Detection/ Silence Suppression	Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.
Comfort Noise Generation	Your device generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).
Echo Cancellation	You device supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
QoS (Quality of Service)	Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. Your device supports Type of Service (ToS) tagging. This allows the device to tag voice frames so they can be prioritized over the network.
Packet Filters	Your device's packet filtering function allows added network security and management.

Appendix B
WiMAX Security

Wireless security is vital to protect your wireless communications. Without it, information transmitted over the wireless network would be accessible to any networking device within range.

User Authentication and Data Encryption

The WiMAX (IEEE 802.16) standard employs user authentication and encryption to ensure secured communication at all times.

User authentication is the process of confirming a user's identity and level of authorization. Data encryption is the process of encoding information so that it cannot be read by anyone who does not know the code.

WiMAX uses PKMv2 (Privacy Key Management version 2) for authentication, and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Protocol) for data encryption.

WiMAX supports EAP (Extensible Authentication Protocol, RFC 2486) which allows additional authentication methods to be deployed with no changes to the base station or the mobile or subscriber stations.

PKMv2

PKMv2 is a procedure that allows authentication of a mobile or subscriber station and negotiation of a public key to encrypt traffic between the MS/SS and the base station. PKMv2 uses standard EAP methods such as Transport Layer Security (EAP-TLS) or Tunneled TLS (EAP-TTLS) for secure communication.

In cryptography, a 'key' is a piece of information, typically a string of random numbers and letters, that can be used to 'lock' (encrypt) or 'unlock' (decrypt) a message. Public key encryption uses key pairs, which consist of a public (freely available) key and a private (secret) key. The public key is used for encryption and the private key is used for decryption. You can decrypt a message only if you have the private key. Public key certificates (or 'digital IDs') allow users to verify each other's identity.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The base station is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your base station acts as a message relay between the MS/SS and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user authentication:

- Access-Request

  Sent by an base station requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The base station sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the base station and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the base station requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.